

1 CLAIMS

2 What is claimed is:

3 1. A digital signature method comprising the steps of:
4 generating summary text for an electronic document;
5 displaying said summary text on the display screen of
6 a terminal of a signatory;
7 calculating a digest value for said summary text
8 using a function with which a value uniquely representing
9 input data is generated and regeneration of said input
10 data from said value is difficult;
11 encrypting data, including said digest value, using a
12 private key stored in said terminal, and generating a
13 signature value; and
14 generating a signed document including said signature
15 value.

16 2. The digital signature method according to claim 1,
17 wherein said electronic document and said signed document
18 are XML documents, and said summary text is generated
19 using XPath of said electronic document, which is an XML
20 document.

21 3. The digital signature method according to claim 1,
22 wherein said terminal includes a signature template having
23 a variable field, further comprising the steps of:
24 adding said digest value to said variable field of
25 said signature template;
26 employing said function to convert said signature

1 template to which said digest value has been added; and
2 employing said private key to encrypt a value
3 obtained by conversion and generating said signature
4 value.

5 4. The digital signature method according to claim 3,
6 wherein a URI for said electronic document is added to
7 said variable field of said signature template.

8 5. The digital signature method according to claim 3,
9 wherein said signature template is canonicalized using a
10 predetermined algorithm.

11 6. The digital signature method according to claim 1,
12 wherein said function is a hash function.

13 7. A digital signature system comprising:

14 means for generating summary text for an electronic
15 document;

16 means for displaying said summary text on the display
17 screen of a terminal of a signatory;

18 means for calculating a digest value for said summary
19 text using a function with which a value uniquely
20 representing input data is generated and regeneration of
21 said input data from said value is difficult;

22 means for encrypting data, including said digest
23 value, using a private key stored in said terminal; and

24 means for generating a signed document including a
25 signature value obtained by the cryptography.

1 8. The digital signature system according to claim 7,
2 wherein said electronic document and said signed document
3 are XML documents, further comprising:
4 means for generating said summary text using XPath of
5 said electronic document, which is an XML document.

6 9. The digital signature system according to claim 7,
7 wherein said terminal includes a signature template having
8 a variable field, further comprising:

9 means for adding said digest value to said variable
10 field of said signature template;

11 means for employing said function to convert said
12 signature template to which said digest value has been
13 added; and

14 means for employing said private key to encrypt a
15 value obtained by conversion.

16 10. The digital signature system according to claim 9,
17 wherein a URI for said electronic document is added to
18 said variable field of said signature template.

19 11. The digital signature system according to claim 9,
20 wherein said signature template is canonicalized using a
21 predetermined algorithm.

22 12. The digital signature system according to claim 7,
23 wherein said function is a hash function.

24 13. A digital signature method comprising the steps of:
25 a signature demandant transmitting an electronic

1 document to an agent;

2 said agent generating summary text for said
3 electronic document, and transmitting said summary text to
4 a terminal of a signatory;

5 said signatory displaying said summary text on the
6 display screen of said terminal of said signatory;

7 said signatory confirming said summary text, and
8 employing a private key stored in said terminal to
9 digitally sign said summary text or a document
10 corresponding to said summary text;

11 said signatory transmitting, to said agent, a
12 signature value generated by the digital signature;

13 said agent generating a signed document by adding
14 said signature value to said electronic document; and

15 said agent transmitting said signed document to said
16 signature demandant.

17 14. A digital signature system comprising:

18 means for permitting a signature demandant to
19 transmit an electronic document to an agent;

20 means for permitting said agent to generate summary
21 text for said electronic document, and to transmit said
22 summary text to a terminal of a signatory;

23 means for permitting said signatory to display said
24 summary text on the display screen of said terminal of
25 said signatory;

26 means for permitting said signatory to confirm said
27 summary text, and to employ a private key stored in said
28 terminal to digitally sign said summary text or a document
29 corresponding to said summary text;

1 means for permitting said signatory to transmit, to
2 said agent, a signature value generated by the digital
3 signature;

4 means for permitting said agent to generate a signed
5 document by adding said signature value to said electronic
6 document; and

7 means for permitting said agent to transmit said
8 signed document to said signature demandant.

9 15. A digital signature mediation method comprising the
10 steps of:

11 receiving an electronic document from a signature
12 demandant, and generating summary text for said electronic
13 document;

14 transmitting said summary text to a terminal of a
15 signatory;

16 generating a signed document by adding, to said
17 electronic document, a signature value received from said
18 terminal of said signatory; and

19 transmitting said signed document to said signature
20 demandant.

21 16. The digital signature mediation method according to
22 claim 15, wherein said electronic document and said signed
23 document are XML documents, and said summary text is
24 generated using XPath of said electronic document, which
25 is an XML document.

26 17. A digital signature mediation system comprising:
27 means for receiving an electronic document from a

1 signature demandant, and for generating summary text for
2 said electronic document;
3 means for transmitting said summary text to a
4 terminal of a signatory;
5 means for generating a signed document by adding, to
6 said electronic document, a signature value received from
7 said terminal of said signatory; and
8 means for transmitting said signed document to said
9 signature demandant.

10 18. The digital signature mediation system according to
11 claim 17, wherein said electronic document and said signed
12 document are XML documents, further comprising:

13 means for generating said summary text using XPath of
14 said electronic document, which is an XML document.

15 19. An information terminal comprising:

16 means for receiving summary text for an electronic
17 document;

18 means for displaying said summary text on a display
19 screen;

20 means for calculating a digest value for said summary
21 text using a function with which a value uniquely
22 representing input data is generated and regeneration of
23 said input data from said value is difficult;

24 storage means for storing a private key;

25 means for employing said private key to encrypt data,
26 including said digest value; and

27 means for generating a signature value obtained by
28 the cryptography.

1 20. The information terminal according to claim 19,
2 further comprising:
3 storage means for storing a signature template having
4 a variable field;
5 means for adding, to said variable field of said
6 signature template, said digest value, a URI of said
7 electronic document and other information concerning said
8 electronic document;
9 means for employing said function to convert said
10 signature template to which said digest value and said
11 information have been added; and
12 means for employing said private key to encrypt a
13 value obtained by conversion, and generating said
14 signature value.

15 21. The information terminal according to claim 20,
16 wherein said electronic document is an XML document, and
17 said signature template is canonicalized using a
18 predetermined algorithm.

19 22. A digital signature method comprising the steps of:
20 receiving summary text for an electronic document;
21 displaying said summary text on a display screen;
22 calculating a digest value for said summary text
23 using a function with which a value uniquely representing
24 input data is generated and regeneration of said input
25 data from said value is difficult;
26 encrypting data, including said digest value by
27 employing said private key that is recorded in a storage

1 area of an information terminal, or in a storage area of a
2 memory connectable to said information terminal; and
3 generating a signature value obtained by the
4 cryptography.

5 23. The digital signature method according to claim 22,
6 further comprising:

7 adding said digest value, a URI of said electronic
8 document and other information concerning said electronic
9 document to a variable field of a signature template,
10 which that is recorded in said storage area of said
11 information terminal or in a storage area of a memory
12 connectable to said information terminal;

13 employing said function to convert said signature
14 template to which said digest value and said information
15 have been added; and

16 employing said private key to encrypt a value
17 obtained by conversion, and generating said signature
18 value.

19 24. The digital signature method according to claim 23,
20 wherein said electronic document is an XML document, and
21 said signature template is canonicalized using a
22 predetermined algorithm.

23 25. A computer-readable storage medium, on which
24 information for a private key, for public key
25 cryptography, and a program are stored that permit a
26 computer to perform:

27 a function for calculating a digest value for said

1 summary text using a function with which a value uniquely
2 representing input data is generated and regeneration of
3 said input data from said value is difficult;
4 a function for employing said private key to encrypt
5 data, including said digest value.

6 26. An article of manufacture comprising a computer
7 usable medium having computer readable program code means
8 embodied therein for causing a digital signature, the
9 computer readable program code means in said article of
10 manufacture comprising computer readable program code
11 means for causing a computer to effect the steps of claim
12 1.

13 27. An article of manufacture comprising a computer
14 usable medium having computer readable program code means
15 embodied therein for causing a digital signature, the
16 computer readable program code means in said article of
17 manufacture comprising computer readable program code
18 means for causing a computer to effect the steps of claim
19 13.

20 28. An article of manufacture comprising a computer
21 usable medium having computer readable program code means
22 embodied therein for causing digital signature mediation,
23 the computer readable program code means in said article
24 of manufacture comprising computer readable program code
25 means for causing a computer to effect the steps of claim
26 15.

1 29. A program storage device readable by machine,
2 tangibly embodying a program of instructions executable by
3 the machine to perform method steps for a digital
4 signature, said method steps comprising the steps of claim
5 1.

6 30. A program storage device readable by machine,
7 tangibly embodying a program of instructions executable by
8 the machine to perform method steps for a digital
9 signature, said method steps comprising the steps of claim
10 13.

11 31. A program storage device readable by machine,
12 tangibly embodying a program of instructions executable by
13 the machine to perform method steps for a digital
14 signature, said method steps comprising the steps of claim
15 15.

16 32. A computer program product comprising a computer
17 usable medium having computer readable program code means
18 embodied therein for causing a digital signature system,
19 the computer readable program code means in said computer
20 program product comprising computer readable program code
21 means for causing a computer to effect the functions of
22 claim 7.

23 33. A computer program product comprising a computer
24 usable medium having computer readable program code means
25 embodied therein for causing a digital signature system,
26 the computer readable program code means in said computer

1 program product comprising computer readable program code
2 means for causing a computer to effect the functions of
3 claim 14.

4 34. A computer program product comprising a computer
5 usable medium having computer readable program code means
6 embodied therein for causing a digital signature mediation
7 system, the computer readable program code means in said
8 computer program product comprising computer readable
9 program code means for causing a computer to effect the
10 functions of claim 17.

11 35. A computer program product comprising a computer
12 usable medium having computer readable program code means
13 embodied therein for causing an information terminal, the
14 computer readable program code means in said computer
15 program product comprising computer readable program code
16 means for causing a computer to effect the functions of
17 claim 19.

18 37. An article of manufacture comprising a computer
19 usable medium having computer readable program code means
20 embodied therein for causing a digital signature, the
21 computer readable program code means in said article of
22 manufacture comprising computer readable program code
23 means for causing a computer to effect the steps of claim
24 22.

25 38. A program storage device readable by machine,
26 tangibly embodying a program of instructions executable by

